

ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY RESOURCES

1. REASON FOR ISSUE: This Directive establishes policy for the acquisition and management of information technology (IT)-related resources across the Department of Veterans Affairs (VA). VA's IT assets are core resources of the Department and their effective management is critical to the provision of services to our Nation's Veterans. This policy clarifies the scope of VA's IT resources subject to the oversight authority of VA's Chief Information Officer (CIO). This oversight is necessary to ensure alignment of these resources with enterprise IT, information management and information assurance policies, rules, standards and guidance. Additionally, this policy ensures that all VA IT-related assets are acquired within the constraints and intent of the VA's IT Systems appropriation account, providing specific guidance as to when IT-related assets must be funded from the IT Systems account and when these assets may be funded from funding sources other than the IT Systems account. All of VA's IT-related assets, regardless of funding source, are subject to enterprise-wide IT policy rules, standards and oversight defined by VA's CIO. This policy, which replaces all previous memoranda on this subject, is necessitated by the growing magnitude and speed of change in information technologies, network-attached devices (i.e. the "Internet of Things"), and information security risks, procedures and regulations. Its full implementation will improve VA's effectiveness in the use of resources to deliver a standardized, integrated, interoperable, Veteran-centric information environment, in accordance with all federal laws, regulations, and industry best practices.

2. SUMMARY OF CONTENTS: This Directive affirms the VA CIO's oversight authority over all VA IT-related assets as highlighted by the Federal Information Technology Acquisition Reform Act (FITARA), and establishes roles and responsibilities among VA administrations and staff offices, including the Office of Information & Technology (OI&T).

- a. Specifies that an IT-related asset is any VA asset, resource, or service that creates, stores, transmits, manipulates, or displays information, and that it shall comply with laws, executive mandates, and all VA CIO policies, regardless of the funding source. These VA CIO policies include: IT capital planning and investment control investment management and acquisition; information assurance, security and privacy; enterprise architecture, standards and specifications; and IT management, technical and operational controls.
- b. Provides guidance and principles on the use of the VA IT Systems appropriation and other VA appropriations, for the acquisition, development, and operation of VA IT assets in a secure, consistent, effective and efficient manner, as directed by congressional authority.
- c. Rules and standards relative to enterprise-wide management of IT resources are published as part of VA's Enterprise Architecture and governed by the IT Planning, Programming, Budgeting and Execution Board (IT PPBEB) and IT Leadership Board (ITLB).

- 3. RESPONSIBLE OFFICE:** Department of Veterans Affairs Chief Information Officer (CIO).
- 4. RELATED HANDBOOK:** None
- 5. RESCISSION:** Any memoranda written prior to this Directive that authorizes the acquisition of IT resources by an organization other than the Office of Information and Technology. In addition, the following memoranda are rescinded:
- a.** Use of the Information Technology (IT) Systems Appropriation, dated June 21, 2006
 - b.** Use of Medical Care Funds to Develop Mobile Device Applications for Clinical Support, dated May 31, 2011
 - c.** Use of Medical Care Funds for Development, Procurement and/or Support of Mobile Health Applications and Supporting Mobile Devices, dated July 16, 2013

Certified By:

/s/
LaVerne H. Council
Assistant Secretary for
Information and Technology

**BY DIRECTION OF THE DEPUTY
SECRETARY OF VETERANS AFFAIRS:**

/s/
LaVerne H. Council
Assistant Secretary for
Information and Technology

Distribution: Electronic Only

August 31, 2016

ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY ASSETS

1. PURPOSE AND SCOPE. This Directive establishes policy for the development, acquisition, operations and management of information technology (IT) assets across the Department of Veterans Affairs (VA). VA's IT assets are core resources of the Department, and their effective management is critical to VA's ability to deliver uniform, seamless, secure and integrated capabilities to Veterans and their dependents, VA employees and VA's strategic business partners. This Directive will provide the policy necessary to ensure proper stewardship of federal IT resources.

a. The boundaries of what is "IT" are becoming increasingly blurred. In the emerging "Internet of Things" and "consumerization of IT", almost every device or object within VA's operating environment potentially has the ability to communicate with VA's information networks. This goes well beyond the traditional concept of IT (computers, networks, application systems, etc.) to encompass medical devices, radio frequency identification inventory tags, mobile devices, industrial control systems, devices owned and operated by VA staff and Veterans themselves and other assets, all of which contribute to the richness and complexity of VA's information environment. While this evolution has created vast opportunities for greater visibility into and more effective management of VA's operations, it has also resulted in substantial challenges in the management of vast amounts of new information and the security of the overall environment.

b. As the statutorily accountable official for the management and security of all of VA's information resources, including VA operational information and associated resources such as personnel, equipment, funds, and IT, VA's Chief Information Officer (CIO) has authority over all information-related assets that are part of or interact with VA's information networks, services and capabilities. This policy:

- (1) Clarifies the scope of VA's IT assets.
- (2) Specifies that any VA asset, resource, or service that stores, transmits, manipulates or displays VA information shall comply with all laws, executive mandates and VA CIO policies regarding IT, such as capital planning and investment control; investment management and acquisition; information assurance, security and privacy; enterprise architecture, standards, and specifications; and IT management, technical and operational controls, regardless of the funding source.
- (3) Affirms that all VA IT assets, regardless of how funded or managed, are subject to rules, standards and oversight processes as prescribed by the VA CIO. This policy clarifies and strengthens the ability of the VA CIO to manage enterprise compliance with value measurement, architecture, accessibility and information assurance standards, in accordance with congressional intent and the highest standards of public transparency and resource stewardship.

- (4) Ensures that all IT-related assets within VA are developed, procured and operated in the most effective and efficient manner possible within the confines and intent of VA appropriations and other relevant information resource management laws, regulations, executive orders and OMB circulars.
- (5) Defines the circumstances under which IT-related assets must be developed, acquired or operated with the OI&T appropriations and those circumstances under which they may be acquired by VA organizations and facilities with other funds.
- (6) Assigns roles and responsibilities related to the funding and management of VA's IT resources.
- (7) Specifies that acquisition of all IT-related assets shall be strictly limited to contract vehicles authorized by the VA CIO in order to assure proper adherence to VA IT policies such as cybersecurity and accommodation for persons with disabilities.
- (8) States that user privilege levels shall be managed exclusively by OI&T.
- (9) States that configuration and maintenance of end user devices, irrespective of funding source, shall be managed by OI&T.
- (10) States that on-going maintenance for devices funded outside the IT Systems appropriation shall be funded from the original funding source, but executed solely by OI&T.
- (11) Updates governance of IT-related assets, operating guidelines and definitions.
- (12) Provides implementation direction that addresses timely reporting of benefits, costs, budgets and statuses of all VA IT programs as well as full visibility into all VA IT-related assets and resources.
- (13) Reinforces VA's use of life cycle management and total cost of ownership in the planning and management of all IT-related assets and services planned for or deployed in VA.

2. POLICY

- a. All VA information resources (including all information collected, acquired, manipulated, or stored by the Department in the course of conducting VA business and in serving VA customers) are critical VA assets and shall be managed to provide the most secure, integrated, efficient and effective service to VA stakeholders and customers in accordance with this policy, applicable laws and executive orders.
- b. All VA assets, resources, or services that store, transmit, manipulate, or display VA information shall comply with all laws, executive mandates and VA CIO policies regarding IT-related assets, such as capital planning and investment control;

investment management and acquisition; information assurance, security and privacy; enterprise architecture, standards and specifications; and IT management, technical and operational controls, regardless of the funding source.

c. VA defines “information technology” consistent with section 11101 of title 40, United States Code terms. To further clarify, VA considers any device, system, service or capability that connects to VA’s IT networks to create, use, update or delete information electronically to be IT (synonymous with “IT-related asset”). Additionally, VA classifies any capability or service (developed or acquired) that provides electronic information that must be interoperable with VA operating data as IT (synonymous with “IT-related asset”).

d. The IT Systems appropriation shall be used to develop, acquire, operate and maintain all VA IT Systems, both enterprise and locally-unique, including infrastructure and data management services, to ensure proper and uniform operations across all organizational boundaries of VA Administrations and staff offices except as provided in section 3 h below.

e. The IT Systems appropriation shall be used when the product or service is an authoritative data source, system of record or when the product or service updates permanent (i.e., persistent, non-volatile) data stores, whether designated as authoritative or not. This policy excludes medical devices that do not transmit, store or display information. CIO management of the persistent data stores improves mission effectiveness by eliminating duplicative data sources, ensuring data standardization, quality, security and enabling reuse and interoperability.

f. Any use of funding outside of the IT Systems appropriation for IT-related assets and activities must be approved by the VA CIO and may require congressional approval through a reprogramming notification.

g. The following shall be funded with the IT Systems appropriation:

(1) All IT networks.

(2) Development, acquisition, product support and management of software applications, including any open source, innovation, and pilots, mechanisms and services for providing access to applications (e.g. mobile app store) in any IT environment operating under VA control, including private/commercial cloud operations.

(3) IT infrastructure (e.g., servers, storage, networks) required to maintain persistent data sources, both authoritative and non-authoritative, and legacy stores, including all data storage, backup and disaster recovery capabilities.

(4) Voice, data, and video telecommunications infrastructure (e.g., circuits and switches, wired cabling to the wall), regardless if the space is owned or leased by VA.

(5) Telecommunications and telephony usage charges.

(6) All software licenses, enterprise and unique, with the exception of biomedical and clinical software, which must follow the Exemption Approval Process listed in the Appendix. Any biomedical and clinical software that is excepted through the Exemption Approval Process must comply with all OI&T operational and security requirements.

(7) IT system administration training.

(8) IT development and testing environments and performance testing.

(9) IT life cycle planning, technical requirements gathering (not business requirements) and definition, and evaluation as necessary and incidental to the development, acquisition and operation of IT systems.

(10) End User Support Center operations for IT capabilities operated by VA.

(11) Leased space or non-VA furnished space occupied by OI&T employees whose salaries are paid by the IT Systems appropriation, not to include new construction.

(12) All IT costs in support of VA mission-related operations incurred by VA Franchise Fund Enterprise Centers under OI&T management.

(13) IT related services required to initially establish VA Revolving Funds (e.g., Supply Fund, Canteen Fund, Franchise Fund and insurance accounts). Subsequent IT related services and operations and maintenance costs will be reimbursed to OI&T by the fund.

(14) Subscriptions and other service models used in VA's IT production environment such as infrastructure- (IAS), platform- (PAAS), and telecommunications-as-a-service, as defined by National Institute of Standards and Technology's (NIST) guidelines, that require VA maintenance and/or interfaces to VA IT production environment, applications or data stores.

h. This policy allows for flexibility in phased implementation of proper architecture and management controls for devices to take advantage of economies of scale, assure cybersecurity, 508 compliance and adoption of industry best practices. However, all VA assets, resources or services that store, transmit, manipulate or display VA information, or are connected in any way to the VA network, shall comply with all laws, executive mandates and VA CIO policies, such as IT capital planning

and investment control; investment management and acquisition; information assurance, security and privacy; enterprise architecture, standards and specifications; and IT management technical and operational controls, regardless of the funding source. If proper VA CIO and acquisition processes are not followed, the responsibility is with the buyer. The following items may be funded with VHA, VBA, NCA or Staff Office funds:

(1) Medical devices and equipment that communicate with VA IT networks. Medical devices, equipment and mobile medical apps that:

(a) Directly interface with the patient for purpose of physiologic monitoring, processing of human tissue or imaging of the human body; or

(b) Directly connect to the patient for the purpose of fluid resuscitation or pharmaceutical delivery; or

(c) Any other medical devices that transmit, store, or receive data.

(2) Non-IT consumables (e.g. privacy screens, wireless keyboards and mouse pads) for end-user devices.

(3) Applications end-user business process re-engineering.

(4) Software-as-a-Service (SaaS) solutions that follow the Exemption Approval Process as outlined in the Appendix.

(5) High capacity multifunction devices that have copying, emailing and/or printing capabilities within one device and support a large office or workgroup.

(6) Facility management and industrial control equipment, such as fire alarm, building security, energy efficient lighting monitors/transmitters and elevator systems.

(7) Construction projects, including modifications to a building's infrastructure even though required specifically for IT purposes. Examples include: the acquisition and installation of a wire closet fiber optic infrastructure, power surge protection, distribution and battery backup systems, and heating, ventilation and air conditioning (HVAC) equipment to comply with either operating requirements and/or manufacturer warranties. This includes construction of data centers. The IT appropriation does not have the legal authority to incur any construction costs.

(8) Initial costs of IT-related assets and services funded by grants or other non-VA funding sources, such as research efforts.

(9) IT-related assets for delivery to Veterans provided by benefits programs under Title 38 authorities.

(10) Any request outside of the standard configuration must follow the Exemption Approval Process as outlined in the Appendix, or, if applicable, the reasonable accommodation process as specified in VA Handbook 5975.1, Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities.

i. This Directive applies to all VA administrations, staff offices, and all other entities within VA, no matter the source of funding or appropriation. It applies to all planning, development, operations, rules, requirements and standards related to the origination, display, capture, use, processing, transmission and storage of information.

j. The Department's legacy IT-related products and services represent significant challenges. This Directive requires all legacy IT-related services and products to be brought into compliance with this policy regardless of the initial appropriation used to procure or develop the product or service, including funding through reimbursement mechanisms.

k. Nothing in this Directive alters or supersedes the duties and responsibilities identified in the References section.

l. Deadlines for Activities Operating Outside of Scope of this Directive

(1) Within 60 days of the signing of this policy, any initiative, project or effort that is currently out of scope of this Directive should contact your IT Account Manager who is to understand the software (its use, costs, etc) and discuss the next steps with the business partner after briefing and discussions with the CIO.

(2) Within 90 days of the signing of this policy, any initiative, effort or project that did not alert the IT Account Manager will stop all development and work.

m. Exemption Approval Process

(1) Software as a Service (SaaS) and any other proposed IT-related acquisitions that seek to use funding outside of IT Systems appropriation may be granted exemption from this Directive on a case by case basis with a written business case justification that goes through the following approval chain:

- a. IT Account Manager's Office
- b. Office of Information Security
- c. 508 Compliance
- d. Enterprise Program Management Office (EPMO)

(2) All IT-related acquisitions that use funding outside of IT Systems appropriation are subject to the annual certification letter signed by the OI&T CFO or Senior Executive Leadership of each VA administration and staff office.

3. RESPONSIBILITIES.

a. The Office of Information and Technology (OI&T). In planning, managing and overseeing the VA's information resources OI&T shall:

(1) Plan, program, budget and execute the IT Systems appropriation.

(2) Manage approved reimbursable budget transfers when required to move the applicable funding between affected organizations.

(3) Design, develop, implement and maintain a VA IT governance structure to: 1) ensure the proper use of the IT appropriation and acquisition of VA enterprise IT capabilities, and 2) ensure all VA information resources, including those funded outside the IT appropriation, are compliant with enterprise policy, rules, standards and guidance related to IT, IM and information security throughout the PPBE cycle.

(4) Approve all use of non-IT funds for IT-related assets and services.

(5) Provide visibility through the VA's enterprise architecture to all policy, rules, standards, guidance and configurations necessary to guide and constrain VA IT-related design, acquisition, development and deployment.

(6) Develop, maintain, and assure completeness and proper use of standard configurations.

(7) Establish and maintain bulk buy and enterprise purchase programs for IT-related assets (including assets such as end user devices which may be purchased outside the IT appropriation) and services to ensure standardization, interoperability, economies of scale and accessibility of the VA information environment.

(8) Oversee and collaborate with VA stakeholders at the local level to ensure that IT-related capabilities funded and deployed at local sites are appropriately vetted and formally approved through OI&T's Enterprise Program Management Office (EPMO). Ensure alignment to enterprise policy, rules, standards and guidance. Ensure that acquisitions are available to all other local sites and not redundant, while making certain that operations and sustainment are properly funded and the proper appropriation is used.

(9) Integrate compliance with this policy within decision processes that OI&T oversees or participates in.

b. VA Administrations and Staff Offices. As part of their mission responsibilities,

the VA administrations, staff offices and those who support them shall:

- (1) Ensure that all use of non-IT funds for IT-related assets and services is approved by VA OI&T.
- (2) Ensure compliance with laws, executive mandates and VA CIO policy regarding IT capital planning and investment control, investment management and acquisition; information assurance, security and privacy; enterprise architecture, standards and specifications; and IT management, technical and operational controls. This applies to any VA asset, resource or service that stores, transmits or displays VA information, regardless of the funding source.
- (3) By September 1st of each year, submit an annual IT-related acquisition funding and disposal plan for the next fiscal year. The plan will contain planned solicitation and award dates, costs, funding sources, project management points of contact and the number of VA components to which the procured assets or services are applicable. Note: If two or more business units can use the proposed solution then it is considered to be an enterprise solution.
- (4) Estimate and measure the value of proposed IT functionality.
- (5) Conduct all business process reengineering of workflow processes to ensure that the value proposition for the IT investment is realized.
- (6) Maximize collaboration with the open source IT community.
- (7) Participate in the full system development life cycle (SDLC) for new products, including Integrated Project Team (IPT) membership, robust design, test and evaluation of new IT capabilities.
- (8) Plan, program and budget for IT resources limited to and consistent with this policy. There shall be no development, acquisition or operation of IT-related capabilities outside the scope of this policy
- (9) Collaborate and participate in the VA IT governance structures/bodies responsible for determining compliance with the conditions and principles on the proper use of the IT appropriation and acquisition of all VA IT capabilities, both enterprise and local.
- (10) Advocate for proper usage of the IT appropriation in mission-specific areas consistent with the conditions and principles in this policy.
- (11) Ensure that all purchases of IT-related products and services made with non-IT funds in accordance with this policy leverage all available enterprise purchasing agreements. In the absence of an available enterprise agreement, ensure that purchases are bundled such that the best value acquisition strategy can be pursued.

(12) Ensure that all IT-related assets, services, and purchasing functions are appropriately managed and compliant with this policy, including all enterprise IT, IM and information security policy, rules, standards and guidance, regardless of funding source.

(13) Integrate compliance with this policy within established decision processes in which they oversee or participate.

4. REFERENCES

- a. Federal Information Technology Acquisition Reform Act: Title VIII, Subtitle D of the National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291
- b. 29 USC 794d : *Disabled VA Employees and Members of the Public*
- c. 40 USC §11101, *Definitions* and SUBTITLE III: *Information Technology Management, and The Clinger-Cohen Act of 1996*
- d. 44 USC: *Information Resources Management*
- e. Title VIII, Subtitle D of the National Defense Authorization Act (NOAA) for Fiscal Year 2015, Pub. L. No. 113-291, *December 19, 2014: Federal Information Technology Acquisition Reform Act (FITARA) of 2014*
- f. 44 USC 35, Dec 2014: *Federal Information Security Modernization Act of 2014 (FISMA)*
- g. Public Law 107-347, December 2002: *E-Government Act of 2002*
- h. Public Law 109-114, November 30, 2005: *Military Quality of Life and Veterans Affairs Appropriations Act*
- i. 38 USC §§ 5705, 5701 and 7332: *Protection of Medical Records*
- j. 44 USC 3501-3521: *Paperwork Reduction Act of 1995 (PRA)*
- k. PL 111-352, Jan 2011: *Government Performance Results Act (GPRA) of 2010*
- l. OMB Memorandum M-15-14, June 10, 2015: *Management and Oversight of Federal Information Technology*
- m. OMB Circular No. A-11: *Preparation, Submission, and Execution of the Budget*
- n. OMB Circular No. A-130, *Management of Federal Information Resources*
- o. Consolidated Appropriations Act, 2002, S-515, *Information Quality Act (also known as the Data Quality Act)*
- p. OMB Memorandum M-11-29, Aug 2011: *Chief Information Officer Authorities*
- q. OMB Memorandum M-12-18, *Managing Government Records Directive*, Aug 2012
- r. OMB Memorandum (M-06-16) *Protection of Sensitive Agency Information* (June 23, 2006)

- s. OMB Memorandum (M-15-14) Management and Oversight of Information Technology
- t. VA Directive 6300, February 26, 2009: *Records and Information Management*
- u. VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*

5. DEFINITIONS

a. Adequate Security. (See OMB A-130 Circular A-130 Appendix III) Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity and availability, through the use of cost-effective management, personnel, operational and technical controls.

b. Application. (See OMB Circular A-130 Appendix III) The use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. Authoritative Data Source. A source of data or information designated and recognized as official that is trusted, timely, secure and used within VA's information environment in support of VA business processes. An authoritative data source is the one and only (logical) location where a respective data element is created, updated and deleted. Administrations and staff offices designate these sources within domains for which they are the stewards. The Office of Information and Technology develops and maintains technology solutions (e.g. services) that use these sources. [VAD 6518 EIM Policy]

d. Authorized User. A person who is granted access to information resources based upon permission, need-to-know, organization security policy, and federal security and privacy laws.

e. Business Unit. A program office or organization under one of VA's Administrations or a corporate function.

f. Capability. The ability to achieve a desired effect under specified [performance] standards and conditions through combinations of ways and means [activities and resources] to perform a set of activities.

Alternate Definition: A capability is an organization's desired or existing set of assets that enables contribution to an objective or outcome outlined by the organization. Capabilities typically require a combination of people, process, policy and technology elements. [VAECM 1.0]

g. Common Information. Information that is used by multiple components across the VA enterprise to conduct business. Examples of such information include, but are not limited to:

- (1) Identity
- (2) Military Service Record
- (3) Contact Information
- (4) Demographic and Socio-economic.

h. Critical infrastructure and key assets. IT related resources and services required to maintain continuity of operations and integrity of VA's mission operations.

i. Data. An elementary description of things, events, activities and transactions that are recorded, classified and stored, but may not be organized to convey any specific meaning. Data items can be numeric, alphabetic, figures, sounds or images. A database consists of stored data items organized for expeditious use, including reading, updating and deleting.

j. Data Assets. The actual (implemented) data and specific values themselves as well as the repositories, capabilities and services that access, process and store the data.

k. Data Store. Any store of data intended to be persistent (i.e., non-volatile) or leaves residual memory trace of information for the purpose of later processing (creation, reading, updating or deleting), irrespective of its designation as authoritative or relation of a System of Record.

l. Duplicative Information Sources. Multiple information stores of the same Information that is in no way synchronized and/or reconciled with one another.

m. Direct Patient Care. Care of a patient provided personally by a staff member. Direct patient care may involve any aspects of the health care of a patient, including treatments, counseling, self-care, patient education, and administration of medication.

n. IT Capability. A coherent set of resources (IT tools and products) that provide the means by which a task can be performed. IT capabilities are built using any resources and data that are used in one or more localities within the enterprise, but not necessarily at all localities. Within the VA this includes all IT-related services for Veterans and eligible beneficiaries, support functions and resource management. Embodied in this concept are technical efforts such as infrastructure engineering for building, managing and evolving IT; IT infrastructure operations for administering and monitoring the performance of the IT service provided to the local entity; and IT services management.

o. Enterprise IT Capabilities. Enterprise level IT capabilities built using IT resources and data that are shared across two or more organization components regardless of location. Within the VA this includes all IT related services for Veterans and eligible beneficiaries, support functions and resource management. Embodied in this concept are technical efforts such as infrastructure engineering for building, managing and evolving shared IT; IT or infrastructure operations for administering and monitoring the performance of the IT service being provided to the enterprise; and IT services management. Efforts such as IT strategy, portfolio management and IT governance enable this concept to function effectively.

p. General Support System. (See OMB Circular A-130 Appendix III) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people. Some examples of systems are: a local area network (LAN) including smart terminals that supports a branch office; an agency-wide backbone; a communications network; a departmental data processing center including its operating system and utilities; a tactical radio network or shared information processing service organization.

q. Government Information. Information created, collected, processed, disseminated or disposed of, by or for the Federal Government or any other level of government.

r. Information. Any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms. This definition includes information that an agency disseminates from a web page.

s. Information Environment. The aggregate of the information created and used by an organization; the information architecture of the organization (models, authoritative and redundant data stores, data flows); the governance framework and policies and standards that ensure information is managed as an asset.

t. Information Life-Cycle. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

u. Information Management. The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

v. Information Resources. (See 44 USC Section 3502) Information and related resources, such as personnel, equipment, funds and information technology.

w. Information Resources Management. (See 44 USC Section 3502) The process of managing information resources to accomplish agency missions and to improve

agency performance, including through the reduction of information collection burdens on the public.

x. Information System. (See 44 USC Section 3502) A discrete set of information resources organized for the collection, processing, maintenance, transmission and dissemination of information in accordance with defined procedures, whether automated or manual.

y. Information Technology. (See 40 USC Section 1110)

(a) With respect to an executive agency; any equipment, interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. This includes if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use:

- (1) of that equipment; or
- (2) of that equipment to a significant extent in the performance of a service or the furnishing of a product.

(b) Includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(c) Does not include any equipment acquired by a federal contractor incidental to a federal contract.

z. Infrastructure. The substructure or underlying foundation, platform or network used for providing goods and services, including communications facilities, cable, wiring, data centers, power plants and communication systems.

aa. Infrastructure as a Service (IaaS). The capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run any software, which can include operating systems and applications. The consumer manages or controls the underlying cloud infrastructure through contracting mechanisms, but has direct control over operating systems, storage and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

bb. IT Infrastructure. The term IT Infrastructure is applied to a group defined by OMB Circular A-11 Section 300 to include Infrastructure, Office Automation, and Telecommunications. These are defined in OMB A-11 Section 300 as "... all IT investments that support common user systems, communications, and computing

infrastructure. These investments usually involve multiple mission areas and might include general LAN/WAN, desktops, data centers, and cross-cutting issues such as shared IT security initiatives and telecommunications.” [OMB A-11; Section 300]

cc. IT Network. The grouping of two or more computer systems that are physically or virtually linked together.

dd. IT Project. Includes projects for software development, mobile applications, hardware installations, network upgrades, cloud computing/external hosting and virtualization rollouts, enterprise architecture, information assurance, business analytics, data management projects and the implementation of IT services.

ee. IT Service Management. The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology. [ITIL V3.0]

ff. Legacy Systems. Those systems in existence and production at the start of a modernization program.

gg. Major application. (See OMB Circular A-130 Appendix III) An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

hh. Medical Device. Devices that are used for direct physiologic monitoring; tissue processing or imaging of the human body; direct pharmaceutical delivery to the patient (IV, transdermal, automated pill counters and other point of use inventory solutions); or are intended to directly affect the structure or any function of the body (i.e. prosthetic devices).

ii. Multi-Function Device. A device that has copying, emailing and/or printing capabilities within one device and supports a large office or workgroup.

jj. Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer manages or controls the underlying cloud infrastructure including network, servers, operating systems, or storage through contract.

kk. Redundant information. Multiple information stores of the same information that are synchronized and/or reconciled with one another for availability, integrity and continuity purposes.

ll. Service. A mechanism to enable access to a set of one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description or contract.

mm. Software as a Service (SaaS). The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer manages or controls the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities through contract mechanisms, with the possible exception of limited user-specific application configuration settings.

nn. Software Framework. An architecture and development environment that is used to write applications and, often, run them. It includes software tools such as GUI builders, compilers, class libraries and utilities for developing the applications, as well as, in some cases, a runtime engine for executing the applications. It is also sometimes referred to as an application platform. [VASI]

oo. Software Development. The activity of computer programming, documenting, testing and bug fixing involved in creating and maintaining applications and software frameworks involved in a System Development Life Cycle (SDLC) and resulting in a software product. While the term refers to a process of writing and maintaining the source code, in a broader sense it includes all that is involved between the conception of the desired software through to the final manifestation of the software, ideally in a planned and structured process. Therefore, software development may include research, new development, prototyping, modification, reuse, re-engineering, maintenance or any other activities that result in software products. All software development in the VA, whether Class 1, 2 or 3, shall fall under this policy guidance.

pp. Strategic Asset. A resource that is used by an entity to achieve mission-related outcomes.

qq. System. See *General Support System*.

rr. System Development Life Cycle (SDLC). Is a term used to describe a systematic approach and process for planning, creating, testing, deploying and retiring information systems.

ss. Telecommunications. A universal term that is used for a vast range of information-transmitting technologies such as mobile phones, land lines, VoIP and

broadcast networks. It encompasses the infrastructure of a telecommunications network and includes any lines, apparatuses, towers, antennas, or structures used, or for use in, a telecommunications network. In telecommunications, data is transmitted in the form of electrical signals known as carrier waves, which are modulated into analog or digital signals for transmitting information.

tt. VA Components. All VA administrations, staff offices, and all other organizational entities within the VA.

uu.VA Customers. U.S. service members, Veterans, associated family members and other beneficiaries.

The chart below delineates between the products and services that are procured under IT Systems Appropriation, by OI&T; and may be procured under Non-IT Systems Appropriation, by VHA, VBA, NCA, or Staff Offices.

Products and services that are procured under <u>IT Systems Appropriation</u>	Products and services that may be procured under <u>Non-IT Appropriations</u>
<p>Any device, system, service, or capability that connects to VA's IT networks to create use, update, or delete information. Including:</p> <ul style="list-style-type: none"> -Desktop computers -Laptop computers -Mobile phones -Tablets -Video teleconferencing units -Analog telephones -Voice over Internet Protocol (VoIP) Phones -Servers, routers, and hubs - Intranet and Internet - Development, acquisition, product support and management of software applications, including any open source, innovation, and pilots, mechanisms and services for providing access to applications (e.g. mobile app store) in any IT environment operating under VA control, including private/commercial cloud operations. - IT infrastructure (e.g., servers, storage, networks) required to maintain persistent data sources, both authoritative and non-authoritative, and legacy stores, including all data storage, backup and disaster recovery capabilities. - Voice, data, and video 	<p>The following may be funded with VHA, VBA, NCA, or Staff Office Funds:</p> <ul style="list-style-type: none"> - Medical devices and equipment that communicate with VA IT networks. Medical devices, equipment and mobile medical apps that: <ul style="list-style-type: none"> a. Directly interface with the patient for purpose of physiologic monitoring, processing of human tissue or imaging of the human body; or b. Directly connect to the patient for the purpose of fluid resuscitation or pharmaceutical delivery; or c. Any other medical devices that transmit, store, or receive data. <p>Products and services that may be procured under <u>Non-IT Appropriations (continued)</u></p> <ul style="list-style-type: none"> - Non-IT consumables (e.g. privacy screens, wireless keyboards and mouse pads) for end-user devices. - Applications end-user business process re-engineering. - Software-as-a-Service (SaaS) solutions that follow the Exemption Approval Process as outlined in the Appendix. - Multifunction devices that have copying, emailing and/or printing capabilities within one device. - Facility management and industrial

Products and services that are procured under IT Systems Appropriation (continued)

- Telecommunications infrastructure (e.g., circuits and switches, wired cabling to the wall), regardless if the space is VA owned or leased.
- Telecommunications and telephony usage charges.
- All software licenses, enterprise and unique, with the exception of biomedical and clinical software, which must follow the Exemption Approval Process listed in the Appendix (Section 6)
- IT system administration training
- IT development and testing environments and performance testing
- IT life cycle planning, technical requirements gathering (not business requirements) and definition, and evaluation as necessary and incidental to the development, acquisition and operation of IT systems.
- End User Support Center operations for IT capabilities operated by VA.
- Leased space or non-VA furnished space occupied by OI&T employees whose salaries are paid by the IT Systems appropriation, not to include new construction
- All IT costs in support of VA mission-related operations incurred by VA Franchise Fund Enterprise Centers under OI&T management
- Initial costs associated with provisioning of IT-related services through revolving funds (e.g., Supply Fund, Canteen Fund, Franchise Fund and insurance accounts). Operations and maintenance costs will be subsequently reimbursed to OI&T by the fund

control equipment, such as fire alarm, building security, energy efficient lighting monitors/transmitters and elevator systems.

- Construction projects, including modifications to a building's infrastructure even though required specifically for IT purposes. Examples include: the acquisition and installation of a wire closet fiber optic infrastructure, power surge protection, distribution and battery backup systems, and heating, ventilation and air conditioning (HVAC) equipment to comply with either operating requirements and/or manufacturer warranties. This includes construction of data centers. The IT appropriation does not have the legal authority to incur any construction costs.
- Initial costs of IT-related assets and services funded by grants or other non-VA funding sources, such as research efforts.
- IT-related assets for delivery to Veterans provided by benefits programs under Title 38 authorities.

Products and services that may be procured under Non-IT Appropriations (continued)

- Any request outside of the standard configuration must follow the Exemption Approval Process as outlined in the Appendix or, if applicable, the reasonable accommodation process as specified in VA Handbook 5975.1, Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities.

NOTE: VA assets, resources or services that store, transmit, manipulate or display VA information, or are connected in any way to the VA network, shall comply with all laws, executive mandates and VA CIO policies, such as IT capital planning

<p>Products and services that are procured under <u>IT Systems Appropriation</u> (continued)</p> <p>- Subscriptions and other service models used in VA's IT production environment such as infrastructure- (IAS), platform- (PAAS), and telecommunications-as-a-service, as defined by National Institute of Standards and Technology's (NIST) guidelines, that require VA maintenance and/or interfaces to VA IT production environment, applications or data stores</p>	<p>and investment control; investment management and acquisition; <u>information assurance, security and privacy</u>; enterprise architecture, standards and specifications; and IT management technical and operational controls, regardless of the funding source. When available, enterprise strategic sourcing agreements must be utilized to the maximum extent possible. If proper VA CIO and acquisition processes are not followed, the project will be terminated.</p>
---	---